Random System Information Tool

par Pierre Therrode (Espace de Pierre Therrode)

Date de publication : 26 février 2011

Dernière mise à jour :

Certains éléments, notamment sur la partie registre ne sont pas détaillés/expliqués. Il faut donc un minimum de connaissances sur le fonctionnement du registre et sur le fonctionnement d'un système d'exploitation pour comprendre ce cours.

Random System Information Tool, a été créé après HijackThis par Random/Random justement parce que ce dernier n'évoluait plus et que certaines zones non scannées par HijackThis étaient nécessaires pour une bonne désinfection de certains malware.
Ce logiciel est vraiment un bon logiciel, car il donne de nombreux renseignements. Il ne crée pas de clé dans le registre mais seulement un dossier nommé «rsit» à la racine du disque dur pour y stocker les deux rapports qu'il génère. Il est très simple d?utilisation et ne propose pas de fonction de suppression. Il n?y a donc aucun risque pour l?utilisateur.
Le logiciel Random System Information Tool après son scan génère deux rapports : info.txt, et log.txt. Nous allons analyser en détail ces deux rapports. A noter que si on le lance plusieurs fois, il ne génère plus que le rapport log.txt.

I - Le rapport "log.txt"

Ce rapport se découpe en plusieurs parties

I-A - L'en-tête du rapport de Random System Information Tool

I-A-1 - Exemple

.Logfile of random's system information tool 1.08 (written by random/random) **Version de Random System Information Tool**
.Run by Sayce at 2010-07-24 18:26:54 **Nom de l'utilisateur/date/heure**
.Microsoft Windows XP Édition familiale Service Pack 3 **Version du système d'exploitation**
.System drive C: has 31 GB (84%) free of 37 GB **Taille du disque dur principal/Pourcentage de libre**
.Total RAM: 495 MB (50% free) **Taille de la mémoire vive/Pourcentage de libre**

I-A-2 - Explications

Regardez bien les deux dernières lignes. Ces deux lignes peuvent indique l'espace libre sur le disque, et la mémoire utilisé lors du scan, ces deux lignes peuvent expliquer les ralentissements.

I-B - Le rapport HijackThis

Il s'ensuit un rapport HijackThis entier et normal car Random System Information Tool recherche HijackThis sur le PC, si il n'est pas présent il télécharge HijackThis pour qu'il génère un rapport.
Si un firewall, ou un mauvais accès au net empêche ce téléchargement, la phrase «» apparaît à la place du rapport HijackThis.
Je ne vais pas vous détailler les lignes du rapport HJT : il y a un excellent cours sur **BleepingComputer**.

I-C - Les tâches planifiées

Puis vient une liste intitulée «Scheduled tasks folder», c'est-à-dire des tâches planifiées. Ces dernières permettent d'exécuter automatiquement des tâches à un moment précis. Il faut bien les vérifier car souvent les infections créent des tâches planifiées pour, par exemple, se lancer à certains moments précis, elles portent l'extension .job

I-C-1 - Exemple

C:\WINDOWS\tasks\AppleSoftwareUpdate.job

I-C-2 - Explications

Il y a donc une tâche planifiée présente au chemin indiqué apparemment créée par le logiciel de mise à jour de Apple

I-D - La partie Registre

Ensuite, la partie "*Registry dump*", qui contient une liste de nombreuses clés de registre étant souvent utilisées par les infections.
Je vous recommande de faire très attention à cette partie car elle permet de repérer les fichiers/clés/dossiers créés/modifiés par l'infection et donc de l'éradiquer complètement.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ Browser Helper Objects
.Cette clé liste liste les Browser Helper Object (BHO) c'est à dire des application de type "plug-in" qui, une fois installée, ajoute des fonctionnalités (désirées ou non) à Internet Explorer. Les BHO peuvent être nuisibles, et peuvent modifier le navigateur, comme modifier la page d'accueil, afficher des pop-ups...
.Les BHO sont dangereuses dans le sens ou elles s'installent sur le navigateur, qui est aujourd'hui une pierre angulaire de la sécurité du système (Je vous recommande de lire ceci --> mettre lien DVP).

I-D-1 - Exemple

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{25147105-f2aa-4be2-8a71-ac68a4bfa05c}] C:\WINDOWS\system32\wpyugv.dll [2008-11-12 113664]

I-D-2 - Explications

.La clé habituelle, à laquelle un permettant de reconnaître la Browser Helper Object est ajouté en sous-clé.
.Puis, en données, le fichier .dll de la Browser Helper Object est indiqué, suivi de la date de sa création et de sa taille. Vu le nom aléatoire de la .dll, la Browser Helper Object est infectieuse.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar]
.Cette clé liste toutes les barres d'outils (toolbars en anglais), ces barres d'outils s'ajoutent aux navigateurs, et ajoutent des fonctionnalités supplémentaires. A mon sens ces barres sont la plupart du temps dénuées d'intérêt. Ces toolbars sont souvent proposées lors de l'installation de logiciels.

I-D-3 - Exemple

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar\{EE5D279F-081B- 4404-994D-C6B60AAEBA6D}] - EPSON Web-To-Page - C:\Program Files\EPSON\EPSON Web-To-Page\EPSON Web-To-Page.dll [2005-02-21 368640]

I-D-4 - Explications

.La clé habituelle, à laquelle un **CLSID** permettant de reconnaître la barre d'outils est ajouté en sous-clé. Ensuite vient le nom de la barre d'outils. Puis en données, le fichier .dll de la barre d'outils : ici la barre d'outils appartient à Epson, elle est donc légitime
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
.Cette clé liste les logiciels se lançant via la clé «Run». Cette clé, qui permet de lancer les logiciels au démarrage, est très importante lorsque l?on sait que la majorité des infections se lancent dès le démarrage du PC.

I-D-5 - Exemple

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] "QuickTime Task"=C:\Program Files\QuickTime\qttask.exe [2008-03-28 413696]

I-D-6 - Explications

.En 1ère ligne, on voit la clé Run, puis entre guillemets, la valeur mise sous l'effigie de la clé puis, à droite du «=» se trouve la donnée assignée à la valeur suivie de la date de sa création puis de sa taille.
Pour en vérifier la légitimité, on utilise le fichier - ici "*qttask.exe*" - ou le nom de la valeur "*QuickTime Task*". N'oubliez pas de regarder la date de création : lors d'une infection les fichiers infectieux sont tous créés dans la même période.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
Même chose que précédemment sauf que la ruche change : ici c'est "HKCU" Pas d'exemple ici mais c'est la même chose que la précédente ; seule la ruche change.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\]
Liste les services qui se lancent lors du démarrage en mode sans échec.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\]
Liste des services qui se lancent lors du démarrage en mode sans échec avec prise ne charge réseau
[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\]
Liste tous les logiciels autorisés par msconfig au démarrage (visible aussi via msconfig dans la ligne de commande Exécuter).
[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupfolder\]
Liste des programmes du dossier démarrage «C:\Documents and Settings\NOMDESESSION\Menu Démarrer \Programmes\Démarrage». Sous XP et sous Vista, «C:\Users\NOMDESESSION». Ce dossier de démarrage permet de lancer un fichier .lnk (raccourci), qui à son tour lance le .exe dont il est le raccourci.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ Winlogon\Notify\]
Liste des fichiers se lançant dès l'ouverture de session.

I-D-7 - Exemple: vtUklijg.dll []

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\vtUklijg]

I-D-8 - Explications

.La 1ère ligne est la clé listée, c'est à dire HKLM/../Notify suivie de «vtUklijg» en sous-clé.
.Puis en 2ème ligne, la donnée assignée à la clé. Ici la clé/donnée est infectieuse. Vous remarquerez qu'il n'y a pas de date entre les crochets, ce qui signifie souvent, mais pas systématiquement, que la clé est orpheline, c'est à dire que la donnée n'existe pas et qu?en conséquence, la clé ne renvoie vers rien.
Mais le fait que les crochets soient vides peut être dû à un mauvais accès au fichier ou autre.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ ShellServiceObjectDelayLoad]
Liste des fichiers lancés par Explorer.exe
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ System]
Liste des restrictions/stratégies de sécurité. Ces restrictions peuvent être utilisées par les administrateurs dans certains lieux de travail pour empêcher l'accès à certaines options du PC mais elles sont aussi souvent utilisées par les malwares pour empêcher l'accès à la BDR ou au gestionnaire de tâches.

I-D-9 - Exemple: "legalnoticecaption"=

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"dontdisplaylastusername"=1

I-D-10 - Explications

.La première ligne correspond à la clé.
.La deuxième ligne correspond à une restriction nommée "dontdisplaylastusername" qui a pour but de déterminer si le nom du dernier utilisateur doit être conservé pour la prochaine ouverture de la session. Comme vous le voyez, elle a pour donnée "1", le plus souvent (pas systématiquement).
.Lorsque les restrictions ont pour donnée "1" elles sont actives et lorsqu?elles ont pour donnée «0», elles sont inactives.

.La troisième ligne correspond à une restriction nommée "legalnoticecaption". Cette fois, la restriction n?a pas de donnée (souvent les données vides sont les données par défaut).
Ici, les deux restrictions ne sont pas dangereuses mais celle-ci "DisableTaskMgr" permet de désactiver le gestionnaire des tâches et empêche à l?utilisateur d?y accéder. Ceci permet à l?infection d?empêcher l?utilisateur de regarder les processus lancés et donc de vérifier si le PC est infecté.
En conclusion, comme vous le voyez, les restrictions peuvent être intéressantes à utiliser pour les malwares.
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ explorer]
Comme la précédente, seule la dernière sous-clé change. Ici c'est "explorer" au lieu de "system"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\explorer]
Comme la précédente, seule la ruche change : ici c'est "HKCU".
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\ parameters\firewallpolicy \standardprofile\authorizedapplications\list]
Liste les applications autorisées par le firewall de Micosoft. En effet, les applications doivent demander l'accès au net au firewall de Microsoft (s?il est le Firewall du PC) et donc,les malware sont souvent présents dans cette clé du fait qu'ils ont souvent besoin d'avoir un accès au net.

I-D-11 - Exemple -MSN-

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\ firewallpolicy \domainprofile\authorizedapplications\list] "C:\Program Files\Windows Live\Messenger\msnmsgr.exe"="C: \Program Files\Windows Live\Messenger\msnmsgr.exe:*:Enabled:Windows Live Messenger"

I-D-12 - Explications

Cette ligne signifie donc que le logiciel MSN a le droit d'accéder à internet. En effet la première ligne correspond à la clé d'autorisation à l'accès au net ; les autres montrent quels fichiers auront accès au net.
[HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\ mountpoints2\]
Cette clé permet de voir quel périphérique a été connecté au PC et de déceler une infection par support amovible.
Cette clé est très importante!

I-D-13 - Exemple

[HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\mountpoints2\ {410476de-2cf3-11dd-9a4d-001d926d047f}]
shell\AutoRun\command - E:\RavMon.exe
shell\explore\command - E:\RavMon.exe -e
shell\open\command - E:\RavMon.exe

I-D-14 - Explications

.Le CLSID attaché à notre clé de départ est un identifiant propre à chaque support amovible.
.La deuxième ligne correspond au fichier Autorun du support amovible. Le fichier Autorun permet de lancer automatiquement la clé lorsqu'on la branche au PC. C'est via ce fichier que les infections par supports amovibles se propagent.
Ici le fichier s'appelle «RavMon.exe»; une simple recherche sur le net permettra de déterminer qu?il est infectieux.
.La troisième ligne correspond à l'ouverture du support amovible par clic droit / Explorer.
.La quatrième ligne correspond à l'ouverture de support amovible par double-clic gauche.
On en déduit donc que ces supports amovibles sont infectés. Il faudra, par conséquent, lors de la désinfection les brancher au PC afin de les nettoyer.

I-E - Les fichiers/dossiers créés/modifiés

.Vient ensuite la liste des fichiers/dossiers créés "List of files/folders created in the last 1 months", et modifiés "List of files/folders modified in the last 1 months" le dernier mois (réglage par défaut) ou les 2 ou 3 derniers mois. Cette liste permet de repérer les fichiers créés par l'infection depuis leur installation.
.Lors de la liste des fichiers/dossiers créés/modifiés, apparaît en début de ligne la date/l'heure de création du fichier/dossier suivie d?une ou plusieurs lettres qui indique(nt) si c'est un fichier/dossier et les attributs de ce fichier/dossier ; voici les lettres possiblement affichées :
.La lettre "D" pour Directory (Dossier) signifie que l'objet en fin de chemin est un dossier.
.La lettre "S" pour System (Système) signifie que le fichier/dossier est un fichier/dossier système.
.La lettre "H" pour Hidden (Caché) qui signifie que le fichier/dossier est un fichier/dossier caché.
.La lettre "R" pour Read only (lecture seule) signifie que le fichier/dossier est un fichier/dossier en lecture seule.
.La lettre "A" pour Archive (Archive) qui signifie que le fichier/dossier est une archive.
.La lettre "N" pour Normal (Normal) qui signifie que le fichier ne comporte pas d'attribut.

I-E-1 - Exemple -RSH---- C:\WINDOWS\SVCHOST.EXE-

2008-11-12 20:38:26 ----RSH---- C:\WINDOWS\SVCHOST.EXE

I-E-2 - Explications

."2008-11-12 20:38:26" Date et heure de la création du fichier ."RSH" Indique que c'est un fichier système en lecture seule et caché. ."C:\WINDOWS\SVCHOST.EXE" indique le chemin du fichier créé, c'est à dire svchost.exe

I-F - Liste des pilotes et des services

Enfin, pour finir, RSIT nous expose une liste des pilotes "List of drivers" et des services "List of services".
L'état du service/pilote :
La lettre "R" signifie que le service/pilote est démarré (Running)
La lettre "S" signifie que le service/pilote est stoppé (Stopped)
.Le type de démarrage du service/pilote
.Le nombre "0" signifie qu'il est lancé au démarrage du PC
.Le nombre "1" signifie qu'il est lancé au démarrage du système d'exploitation (Windows ...) .Le nombre "2" signifie qu'il est lancé automatiquement .Le nombre "3" signifie qu'il n'est lancé que manuellement. .Le nombre "4" signifie qu'il est désactivé.
Type de ligne Lettre/Chiffre NomRéelDuService(ServiceName);NomDuService(Nomd'usage);;CheminDuFichier [DateDeCréation TailleDuFichier]

I-F-1 - Exemple de service

R2 AntiVirSchedulerService;Avira AntiVir Planificateur; C:\Program Files\Avira\AntiVir Desktop\sched.exe [2009-05-13 108289]

I-F-1-a - Explication

."R2" : Le service est démarré et se lance avec le système.
."AntiVirSchedulerService" : Nom réel du service.
."Avira AntiVir Planificateur" : Nom du service affiché (nom souvent plus simple que le réel)
."C:\Program Files\Avira\AntiVir Desktop\sched.exe" : Fichier exécutable associé au service.
."[2009-05-13 108289]" : Date de création du service (Quand il n'y a pas de date, cela signifie le plus souvent que le fichier n'existe plus). Le chiffre qui suit correspond à la taille du fichier en octets.

II - Le rapport «info.txt»

Celui-ci aussi se scinde en plusieurs parties et nous allons aussi les détailler

II-A - Les logiciels installés

La première partie du rapport se nomme «Uninstall list», et contient la liste des logiciels présents dans Ajout/Suppression de programmes (Sous XP), Programmes et Fonctionnalités (sous Vista/Windows 7).
Cette liste permet de voir s?il y a des logiciels de P2P, des cracks ou encore plusieurs antivirus. Même si l'on aperçoit souvent ces logiciels dans le rapport log.txt, cela permet d'être sûr de tout voir.

II-A-1 - Exemple

La première ligne correspond au logiciel de mise à jour de Apple et indique le fichier exécutable utilisé pour mettre à jour Apple. Ce fichier est un fichier appartenant à Windows permettant de mettre à jour les logiciels fournis avec Windows.
La deuxième ligne nous montre que le logiciel Avast est installé sur le PC. Elle nous montre aussi que le fichier «aswRunDll.exe» lance le fichier "aswRunDll.exe". Il arrive souvent que vous ayez ce genre de ligne dans les rapports HijackThis : **un premier fichier légitime qui en lance un second entre « » qui lui est parfois illégitime**.
En conséquence, lors de la désinfection, si elle est manuelle, ne supprimer que le 2ème fichier.

II-B - Le fichier Host

La deuxième partie nous donne un aperçu du fichier host, nommé «Hosts File». Le fichier Host est un fichier texte qui se trouve ici «%SYSTEMDRIVE%\Windows\Sysem32\drivers\etc\host». Ce fichier texte permet à votre ordinateur de faire la correspondance entre un nom de domaine (google.com) et une adresse IP (216.109.118.69).
En effet, lorsque vous vous connectez à un site web, l'ordinateur utilise ce fichier et ne se connecte pas au site grâce à l'adresse littérale (http://www.google.fr) mais grâce à l'adresse ip (81.905.41.34).
Les fichiers host sont aussi utilisés par les infections car ils peuvent permettre de rediriger les recherches.
En exemple, si vous souhaitiez vous connecter sur le site d'Avira AntiVir pour le télécharger, le malware aura pu modifier le fichier host de telle sorte qu?il vous empêchera l'accès au site web de Avira AntiVir.
Il est donc important de scanner le fichier host, pour déceler tel ou tel détournement de surf.

II-B-1 - Exemple

127.0.0.1 localhost
127.0.0.1 mpa.one.microsoft.com
127.0.0.1 rad.msn.com

II-B-2 - Explications

La première ligne, indique que l'adresse du pc est «127.0.0.1». C'est toujours la même pour tous les PC. Cette adresse est, comme indiqué à côté, l'adresse locale.
La deuxième ligne, indique que l'accès au site « mpa.one.microsoft.com» est bloqué, en effet l'adresse IP « 127.0.0.1» correspond à l'ordinateur.
La troisième ligne, indique que l'accès au site «rad.msn.com» est bloqué, en effet l'adresse IP « 127.0.0.1» correspond à l'ordinateur.

II-C - Le centre de sécurité

La troisième partie «Security center information» ou Centre d?informations de sécurité. Cette partie liste les dernières alertes émises par le centre de sécurité de Windows.

II-C-1 - Exemple

AV: AntiVir Desktop (outdated)

II-C-2 - Explications

Cette ligne nous montre que l'antivirus du PC, - ici Avira AntiVir - n'est pas à jour et que donc le PC court un risque.

II-D - Le journal d'événement

Cette quatriéme partie correspond au «System event log», c'est à dire au journal des événements de Windows.
.Le journal d'événements de Windows permet de lister les événements survenus dans Windows (comme une MAJ de Windows par exemple). Il permet de visualiser les plantages d'applications, les problèmes de périphériques ...
.Le journal d'événements est composé de trois parties :
.Application (événements enregistrés par les applications),
.Sécurité (événements liés aux ouvertures de sessions et à l'utilisation des fichiers),
.Système (événements liés aux composants de Windows) .
.Il existe aussi trois types d'événements :
.Informations (descriptions du fonctionnement normal d'une application ..),
.Avertissement (descriptions d'un événement pouvant entraîner une erreur)
.Erreur (description d'une erreur grave).
Les fichiers journaux se trouvent ici : «%SystemRoot%\System32\Config» (.evt) On peut accéder à l'observateur comme ceci : Cliquer sur démarrer / Exécuter puis inscrivez ceci "eventvwr.msc" » (Sans les "). Je vous laisse consulter ceci (-->mettre lien DVP).

II-D-1 - Exemple

.Type de l'événement : Erreur **"Type d'événement survenu" ici Erreur, niveau maximum de gravité.**
.Source de l'événement : Windows Update Agent **"Application à l'origine de l'erreur"**
.Catégorie de l'événement : Synchronisation logicielle **"Niveau de gravité définie par la source de l'erreur"**
.ID de l'événement : 16 **"Numéro permettant d'identifier le type de l'événement"**
.Date : 26/07/2010 **"Date à laquelle s'est produit l'erreur"**
.Heure : 18:07:42 **"Heure à laquelle s?est produit l'erreur"**
.Utilisateur : N/A **"Utilisateur qui est à l'origine de l'événement"**
.Ordinateur : SAYCE-PC **"Nom du PC sur lequel le problème s?est produit"**
.Description : Connexion impossible, Windows ne parvient pas à se connecter au service Mises à jour automatiques et ne peut donc pas procéder au téléchargement et à l'installation des mises à jour définies par la planification. Windows continuera d'essayer d'établir la connexion. **" Description de l'événement"**

II-D-1-a - Explication

Ceci est une alerte présente dans le journal des événements.

II-E - Les variables d'environnements

La cinquième partie nommée «Environment variables» - ou variables d'environnement- dresse une liste des variables d'environnement présentes sur le PC. Les variables d'environnement sont des variables utilisées par le système d'exploitation pour pointer vers certains chemins.
.En effet, prenons la variable «%temp%» : cette variable pointe vers les dossiers des fichiers temporaires. Les dossiers ne se trouvant pas toujours au même endroit sur les ordinateurs, on utilise cette variable pour être certain de bien supprimer les fichiers temporaires. Si elles n'existaient pas, il faudrait trouver les dossiers temporaires du PC pour ensuite réussir à supprimer les fichiers temp.
Exemple :

La variable «%allusersprofile%» indique le dossier du profil de tous les utilisateurs.
La variable «%ProgramFiles%» indique le dossier des logiciels installés.
La variable «%SystemRoot%» indique l'emplacement des fichiers système... Il en existe bien d'autres; celles-ci ne sont que des exemples. Retenez donc bien que ces variables permettent de pointer vers un endroit précis du disque dur et sont universelles sur les systèmes Windows.
Il est possible de créer des variables d'environnement; il est donc aussi possible aux Malwares de créer leurs propres variables d'environnement. Voilà pourquoi Random System Information Tool nous liste les variables pour nous permettre de voir si des variables infectieuses ont été créées.

II-E-1 - Exemple

"ComSpec"=%SystemRoot%\system32\cmd.exe "TEMP"=%SystemRoot%\TEMP

II-E-2 - Explications

La première ligne signifie que «% ComSpec%» remplace le chemin «C:\WINDOWS\system32\cmd.exe» (En effet, «%SystemRoot%» pointe vers «C:\WINDOWS».
La deuxième ligne montre que la variable «%TEMP%» pointe vers «C:\WINDOWS\TEMP» Cette variable est très utile. En effet, lors d'une désinfection si l'on a besoin de vider les dossiers temporaires, on utilise cette variable.

III - Conclusion

Voilà, c'est la fin de ce cours sur la lecture des rapports de Random System Information Tool. Je n'ai pas intégré de canned sur l'utilisation de RSIT car le net en regorge. A vous de les chercher ou de faire vos propres canneds.

IV - Remerciement

je remercie .....